IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF UTAH

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH jward@thejaawgroup.com THAT IS STORED AT PREMISES CONTROLLED BY Google, LLC.	Case No. 2:24mj257 CMR **Filed Under Seal**

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Special Agent Brandon R. Saliers, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with certain accounts that are stored at premises controlled by Google, LLC. (Google), an email provider headquartered at 1600 Amphitheater Parkway, Mountain View, CA 94043. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A) to require Google to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a Special Agent with the Air Force Office of Special Investigations (AFOSI), at Hill Air Force Base, Utah, and have been since March 2015. As part of my training as a Special Agent, I completed the Criminal Investigator Training Program at the Federal Law Enforcement Training Center (FLETC), Glynco, GA. As a Special Agent of the AFOSI, I am assigned to investigate matters under the jurisdiction of the Department of the Air Force and Department of Defense. My duties include investigating violations of 18 U.S.C. § 1343 (Wire Fraud), 18 U.S.C. § 287 (Criminal False Claim) and 18 U.S.C. § 371 (Conspiracy). During my investigative career I have been the affiant of and have participated in numerous search warrants. During my time investigating these violations, I have had the opportunity to review the fruits of email searches in multiple investigations. In many instances communications are helpful in identifying co-conspirators, methods, and victims.

3. The information in this affidavit is based on my personal knowledge, my training and experience, evidence developed during the investigation, and information obtained from other agents and witnesses. Because the affidavit is submitted for the limited purpose of establishing probable cause in the application of a search warrant, it does not set forth each and every fact that I or others have learned during the course of this investigation.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 1343 (Wire Fraud), 18 U.S.C. § 287 (Criminal False Claim) and 18 U.S.C. § 371 (Conspiracy) have

been committed by Joel Ward (herein identified as Target #1), President, The JAAW Group L.L.C., 7896 South Highland Drive, Cottonwood Heights, UT (herein identified as Target Company) and others. There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband, and fruits of these crimes further described in Attachment B.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the United States … that has jurisdiction over the offense being investigated," 18 U.S.C. § 2711(3)(A)(i), and "is in … a district in which the provider … is located or in which the wire or electronic communications, records, or other information are stored," 18 U.S.C. § 2711(3)(A)(ii).

PROBABLE CAUSE

A. Summary

6. In August 2021, the Target Company was awarded government contract #FA822821C0007 ($3,999,588.22) to install a Baron Weather radar at Patrick Space Force Base/Cape Canaveral, FL. Between September 2020 and April 2022, Target #1 and Becky Lane (herein identified as Target #2) of Target Company, owners of the target email addresses, circumvented the due process of the system outlined in the Federal Acquisition Regulation (FAR). Target #1 and Target Company falsified prices of radar

parts and submitted inflated invoices to the government for payment. The Target Company intentionally omitted $1.3 million worth of spare parts and software requirements from their proposal to avoid competing against other contractors for the award.

7. Target #1 used the target email address, jward@thejaawgroup.com (herein identified as Target #1 Email) and Target #2 used the target email address, blane@thejaawgroup.com (herein identified as Target #2 Email) to communicate on several occasions with the administrators of the government contract.

B. Attempted Conspiracy to commit fraud & wire fraud.

8. In 2021, Target #1 and Target #2 from the defense contractor, Target Company began colluding with government employees Employee #1 and Employee #2 from the 309th Software Engineering Group, Hill AFB, UT. Target Company provided Employees #1 and #2 key documents that should have been exclusively produced by the government during the acquisition process. For example, on January 7, 2021, Target #1 sent an email to Target #2 titled "J&A drafted for [Employee #1]" Target #1 wrote "Please see attached J&A for direct award under FAR authorization to award to SDVOSB [service-disabled veteran owned small business] up to 4M". (Agent Note: The justification and approval (J&A) should be produced solely by the government to justify a sole-source award to a contractor rather than competing the bid which the government prefers.) Employee #1 incorporated Target #1's J&A into the government's records. Employees #1 and #2 skewed the award process to favor a direct award to Target

Company rather than competing the award. Target Company was directly awarded the contract as a Small Disadvantaged Veteran Owned Small Business for $3,999,588.22. FAR paragraph 19.1406 (a)(2)(II) established the maximum direct contract award ceiling at $4 million. Target Company deliberately excluded spare parts and services to remain under the $4 million ceiling to avoid competition.

9. AFOSI agents conducted a search of Employees #1 and #2 and Target #2 government emails based on no expectation of privacy. Numerous suspect emails circulated between Target #1 Email, Target #2 Email, Target #2 government email, and Employees # 1 and #2's government email accounts.

10. On February 14, 2022, Target #2 emailed Target #1 via her government email account to Target #1 Email and wrote the following: "Hi [Target #1], Ok so after much debate and collaboration this morning it was decided to take network items off the list that we are giving to contracting and then absorb that cost and make other Baron parts higher in price. The problem I am running into is that they [government contacting office] are asking for a proposal from Baron on these costs…I have included in the excel sheet for you the cost for [Target Company] and then the cost [Employee #2] is giving to contracting. Can we get a proposal from Baron that states the cost in Line D?" Target #2's email included an Excel spreadsheet titled "Copy of Test Parts [Target Company]14Feb2022". The Excel document listed 28 line items with columns labeled "[Target #1's] Cost" and "Cost". Items listed in the "Cost" column averaged

approximately 40% higher price than "[Target #1's] Cost" items. The total inflated amount was $237,365.42.

11. On February 17, 2022, Target #2 emailed government Employee #2 an email titled "Baron Quote". Target #2 wrote "Please make sure my name is not on the properties…" Attached to the email was a Word document titled "Spare Parts Price Quote Cape Canaveral Feb 2022". The quote listed the same items as the Excel document "Copy of Test Parts[Target Company] 14Feb2022" and listed the inflated prices from the "Cost" column. The properties on the Baron Quote document listed Target #1 as the author.

12. Agents confirmed Target Company submitted the inflated prices to the government which were paid resulting in an unauthorized extra profit of $212,523.72 over the Government negotiated profit of $37,424.88.

13. On March 5, 2024, SA Saliers coordinated with an OSI intelligence analyst to confirm Google hosted Target #1 Email and Target #2 Email via an open source search. SA Saliers submitted a preservation request to Google via the Law Enforcement Request System to preserve Target #1 and Target #2 Emails. Google confirmed the target email addresses and completed the request on March 14, 2024 providing Google Reference Number 54888648.

14. Defense contract projects are often awarded to a contractor through a competitive bid process. Generally, this process occurs when a federal, state, or local entity advertises a project and contractors submit bids in the attempt to be awarded the

project. Your affiant understands this generally referred to as "bid letting." Your affiant understands that typically the lowest and most reasonable bid submitted is selected to complete the work.

BACKGROUND CONCERNING EMAIL

15. In my training and experience, I have learned that Google provides a variety of on-line services, including electronic mail ("email") access, to the public. Google allows users to utilize their own domain for email addresses rather than "@gmail.com," like the email accounts listed in Attachment A. Subscribers obtain an account by registering with Google. During the registration process, Google asks subscribers to provide basic personal information. Therefore, the computers of Google are likely to contain stored electronic communications (including retrieved and un-retrieved email for Google subscribers) and information concerning subscribers and their use of Google services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

16. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying

subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that, even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

17. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (*i.e.*, session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

18. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email

providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

19. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, email communications, contact lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information

may tend to either inculpate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (*e.g.*, location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (*e.g.*, communications relating to the crime), or consciousness of guilt (*e.g.*, deleting communications in an effort to conceal them from law enforcement).

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

20. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Google to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

SEARCH PROCEDURES

21. The initial examination of the electronic information will be performed within a reasonable amount of time not to exceed 120 days from the date of execution of the warrant. If the government needs additional time to conduct this review, it may seek

an extension of the time period from the Court within the original 120-day period from the date of execution of the warrant. The government shall complete this review within 180 days of the date of execution of the warrant. If the government needs additional time to complete this review, it may seek an extension of the time period from the Court.

22. If, at the conclusion of the examination, law enforcement personnel determine that particular files or file folders responsive to this search warrant do not contain any data falling within the scope of the warrant, they will not search or examine those files or folders further without authorization from the Court. Law enforcement personnel may continue to examine files or data falling within the purview of the warrant relating to files or data that fall within the scope of the warrant, through the conclusion of the case.

23. If an examination is conducted, and the electronic information produced in response to this warrant does not contain any data falling within the ambit of the warrant, the government will seal any non-responsive information, absent further authorization from the Court.

24. The government will retain a forensic image of all of the electronic information produced in response to this warrant for a number of reasons, including proving the authenticity of evidence to be used at trial, responding to questions regarding the corruption of data, establishing the chain of custody of data, refuting claims of fabricating, tampering, or destroying data, and addressing potential exculpatory evidence

claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.

CONCLUSION

25. Based on the forgoing, I request that the Court issue the proposed search warrant.

26. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Google. Because the warrant will be served on Google, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,

SALIERS.BRANDON.RUSSELL.1368418826 Digitally signed by SALIERS.BRANDON.RUSSELL.1368418826 Date: 2024.03.14 15:35:51 -06'00'

BRANDON R. SALIERS
Special Agent
U.S. Air Force Office of Special Investigations

Sworn to before me over the telephone and signed by me pursuant to Federal Rule of Criminal Procedure 4.1 and 4(d) on the 14th day of March 2024.

Cecilia M. Romero

HON. Cecilia M. Romero
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with: Target #1 Email, that is stored at premises owned, maintained, controlled, or operated by Google LLC, a company headquartered at 1600 Amphitheater Parkway, Mountain View, CA 94043.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Google (the "Provider")

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved. The Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. The contents of all emails, communications, or messages associated with the accounts from January 1, 2021 to April 30, 2022, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. The types of service utilized;

d. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence, and instrumentalities of violations of 18 U.S.C. § 1343 (Wire Fraud), 18 U.S.C. § 287 (Criminal False Claim) and 18 U.S.C. § 371 (Conspiracy), involving Target #1 Target #2, and Target Company occurring after January 1, 2021 through April 30, 2022, including, for the accounts or identifiers listed on Attachment A, information pertaining to the following matters:

a. Records of communications with other individuals concerning bid rigging, false claims, bribery and conspiracy;

b. Records of communications between Target Company and federal, state, and local agencies regarding administering bid lettings, concerning the bidding process or specific bids that Target Company has submitted;

c. Records of communications between Target Company and Baron Weather Solutions, 4930 Research Dr., Huntsville, AL for accurate pricing information.

d. Photographs and other communications concerning bid rigging, market allocation, wire fraud, and conspiracy;

e. Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;

f. Evidence indicating the email account owner's state of mind as it relates to the crime under investigation;

g. The identity of the person(s) who created or used the user IDs, including records that help reveal the whereabouts of such person(s).

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the Office of Special Investigations may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review. Any search is subject to the search procedures outlined in paragraphs 55-58.